

19TH JUDICIAL DISTRICT COURT FOR THE PARISH OF EAST BATON ROUGE

STATE OF LOUISIANA

NUMBER: 641 928

SECTION: 26

JAMES J. DONELON  
COMMISSIONER OF INSURANCE FOR THE STATE OF LOUISIANA

VERSUS

LOUISIANA HEALTH COOPERATIVE, INC.

COST OK \$ State

NOV 17 2016

FILED: \_\_\_\_\_

DEPUTY CLERK OF COURT

DEPUTY CLERK

Filed on Behalf of - State of Louisiana - State Pays No Court Costs  
La. R.S. 13:4521 and La. R.S. 22:2019

**NOTICE OF DATA SECURITY INCIDENT INVOLVING SUMMIT RE SERVICES, INC. OF OCTOBER 24, 2016 AND LAHC REQUEST FOR COMPLIANCE WITH FEDERAL AND STATE REPORTING REQUIREMENTS AND THE LAHC BUSINESS ASSOCIATE AGREEMENT**

NOW INTO COURT, through undersigned counsel, comes James Donelon, Commissioner of Insurance for the State of Louisiana, in his capacity as Rehabilitator and Billy Bostick, Court appointed Receiver, of Louisiana Health Cooperative, Inc. in Rehabilitation ("LAHC"), who hereby give notice that by letter dated October 24, 2016, LAHC received notice from Summit Reinsurance Services, Inc. ("Summit Re"), a managing general underwriter and reinsurance advisor for healthcare reinsurance, that Summit Re experienced a "data security incident," which was discovered on August 8, 2016, when Summit Re "discovered that ransomware had infected a Summit Re server containing personal information." Summit Re further advised that Summit Re "determined that the information contained on the affected server may consist of one or more of the following data elements: member names, provider names, Social Security numbers, health insurance information, and some claim-focused medical records containing information such as diagnosis/clinical information used by Summit as part of its stop-loss and reinsurance underwriting and consulting services." See attached Exhibit A.

LAHC made demand on Summit Re for full compliance with the reporting requirements of the applicable provisions of the Patient Protection and Affordable Care Act ("ACA") and the implementing sections of the Code of Federal Regulations ("CFR"), the Health Insurance Portability and Accountability Act ("HIPAA"), Louisiana law, including, but not limited to, La. R.S. 51:3071, et seq., and any other such statutory requirements as to a breach of unsecured

protected health information ("PHI") and personally identifiable information ("PII") (all collectively the "Security and Privacy Laws"). See attached **Exhibit B**. It is anticipated that Summit Re will provide the required notices, publication and reporting.

LAHC further provided notice to the United States Department of Health and Human Services ("HHS") and the Centers for Medicare and Medicaid Services ("CMS") of the Summit Re data security incident. See attached **Exhibit C**.

Respectfully Submitted,

BURGLASS & TANKERSLEY, LLC

BY: 

SUE BUSER (#18151)

CELESTE BRUSTOWICZ (#168350)

DENNIS J. PHAYER, ESQ. (#23747)

5213 Airline Drive

Metairie, Louisiana 70001-5602


Phone: (504) 836-2220

Telefax: (504) 836-2221

Attorneys for **JAMES J. DONELON, Commissioner of Insurance for the State of Louisiana as Rehabilitator of Louisiana Health Cooperative, Inc. in Rehabilitation**

#### CERTIFICATE OF SERVICE

I hereby certify that I have not served a copy of the foregoing pleading in these proceedings because there are no other parties in these proceedings, this 15<sup>th</sup> day of November, 2016.





7030 POINTE INVERNESS WAY, SUITE 350 FORT WAYNE, IN 46804  
260.469.3000 • FAX 260.469.3014

October 24, 2016

Privacy Officer  
Louisiana Health Co-op  
3445 N Causeway Blvd #800  
Metairie, LA 70002



RE: Notice of Summit Reinsurance Services, Inc. Data Security Event

Dear Privacy Officer:

We are writing to notify you of a data security event involving Summit Reinsurance Services, Inc. ("Summit"). This event may affect some information belonging to certain individuals affiliated with [Health Plan] and/or your health plan clients. Summit maintains this information as part of Summit's reinsurance and stop-loss underwriting and consulting services it provides to insurance carriers.

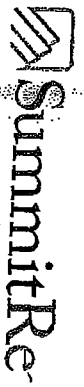
On August 8, 2016, Summit discovered that ransomware had infected a server containing certain personal information. Summit immediately launched an investigation to determine the nature and scope of this event and to prevent the encryption of data contained on the server. Summit also began working with third-party forensic investigators to assist with these efforts. Summit determined that the information contained on the affected server may consist of one or more of the following data elements: member names, provider names, Social Security numbers, health insurance information, and some claim-focused medical records containing information such as diagnosis/clinical information used by Summit as part of its stop-loss and reinsurance underwriting and consulting services.

Summit takes the security of information in our care very seriously. Although our investigation is ongoing, to date we have not found evidence that personal information on the affected server was misused or attempted to be misused. Nevertheless, we are providing you with this notice as information you (or an agent on your behalf) provided Summit was contained on the server under investigation. Upon request, we will securely transfer a file identifying the potentially affected personal information affiliated with your plan. If you would like a copy of this data file, please contact us at [inforesponse@summit-re.com](mailto:inforesponse@summit-re.com) and identify the individual for whom the data file should be transferred and the email address for that individual.

Again, we take the security of personal information in our system very seriously. We apologize for any inconvenience or concern this incident may cause you. We understand that you may have questions that are not addressed in this letter; if you have any questions or concerns, please do not hesitate to contact us at 855-215-0286.

Sincerely,

Mark Troutman  
President



Summit Reinsurance Services, Inc.  
7030 Bolite Inverness Way, Suite 350  
Fort Wayne, IN 46804

7000263729

|||||



02 1P  
0004678960 OCT 24 2016  
MAILED FROM ZIP CODE 46804

\$000.46

# Burglass Tankersley

Attorneys at Law  
5213 Airline Drive  
Metairie, Louisiana 70001-5602  
www.burglass.com

Sue Buser  
sbuser@burglass.com

Direct Dial  
(504) 836-0460  
Direct Fax  
(504) 287-0460

October 31, 2016

Attention: Mark Troutman  
President  
Summit Reinsurance Services, Inc.  
7030 Pointe Inverness Way, Suite 350  
Fort Wayne, IN 46804

CERTIFIED MAIL  
RETURN RECEIPT REQUESTED  
and by regular mail  
and by email to

RE: James J. Donelon, Commissioner of Insurance for the State of Louisiana v.  
Louisiana Health Cooperative, Inc. ("LAHC"), 19th JDC #641 928, Section 26  
Swiss Re Life & Health America, Inc. – Excess Reinsurance Coverage Contract  
(December 27, 2013)  
Business Associate Agreement between Summit Re and Louisiana Health  
Cooperative, Inc. (effective 1/1/14)  
Our File #: 87004

Dear Mr. Troutman:

This firm has been retained to represent the interests of the Louisiana Commissioner of Insurance as the Court-appointed Rehabilitator of Louisiana Health Cooperative, Inc. in Rehabilitation ("LAHC") in the above referenced matter. A copy of the Permanent Order of Rehabilitation of October 21, 2015 is attached.

On October 27, 2016, LAHC received your firm's Notice of Summit Reinsurance Services, Inc. ("Summit") Data Security Event dated October 24, 2016. That notice indicated that Summit discovered that ransomware infected a Summit server containing personal information on August 8, 2016.

A copy of the Business Association Agreement ("BAA") with LAHC, effective September 12, 2013, is attached. As you know, the BAA and 45 CFR 164.410 and 45 CFR 504 require Summit to report a breach of unsecured protected health information ("PHI") and/or individually identifiable health information ("PII") to LAHC without unreasonable delay and in no case later than sixty (60) calendar days after discovery of a breach.

The BAA further provides that Summit report in writing to LAHC any breach of unsecured PHI and/or PII within five (5) business days of the date Summit learned of the incident giving rise to

{00576890 - v1}

the breach and to provide LAHC with the information provided in the Breach Notification Regulations and to reimburse LAHC for any reasonable expenses incurred in the investigation and assessment of the breach and obligations of notification and for reasonable measures taken by LAHC to mitigate harm to affected individuals. BAA section 2.5.

Summit's October 24, 2016 notice to LAHC was not timely as it was given more than five (5) business days after Summit discovered the incident, and more than sixty (60) days after Summit discovered the incident.

Further, Summit's October 24, 2016 notice to LAHC does not provide sufficient information for LAHC to determine if the requirements of 45 CFR 160 and 164 and HITECH have been met by Summit. In fact, Summit's notice does not adequately inform LAHC whether a breach of unsecured PII and/or PHI occurred, and if so, the nature and extent of the PHI and/or PII involved. 45 CFR 160.103, 45 CFR 164.404, 45 CFR 164.501 and 45 CFR 164.502.

At a minimum, Summit is required to provide LAHC with the following:

- 1) Whether the Summit data security event involved PHI and/or PII that had been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology approved by the U.S. Department of Health and Human Services ("DHS") and/or the Centers for Medicare and Medicaid Services ("CMS");
- 2) The nature and extent of the unsecured PHI and/or PII involved, if any, including the types of identifiers and details as to the types of information involved;
- 3) The likelihood of re-identification;
- 4) The unauthorized person or entities who obtained the PHI and/or PII;
- 5) Whether the PHI and/or PII was actually acquired or viewed;
- 6) The probability that the PHI and/or PII has been compromised;
- 7) The extent to which the risk to the PHI and/or PII has been mitigated;
- 8) Whether Summit has and/or plans to provide notice of the breach to each individual whose PHI and/or PII has been or is reasonably believed to have been accessed, acquired, used and/or disclosed as a result of the breach;
- 9) Any steps affected individuals should take to protect themselves from potential harm resulting from the breach;
- 10) Whether Summit plans to notify DHH, CMS, the U.S. Federal Trade Commission, and the media as to the breach;
- 11) The date of the breach and a description of what happened;
- 12) A detailed description of what Summit is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches, including, but not limited to the findings of the third party forensic investigators Summit has retained to investigate and report on the breach;
- 13) The steps Summit plans to take to comply with all federal and state requirements as to notice of the breach of secured PHI and/or PII and the adequacy of these steps under applicable federal and state law and regulations.

I also reiterate the requests made by the LAHC Security Officer Philip D'Antonio by email on October 28, 2016, as follows:

- a) Was LAHC PHI or PII stored in an encrypted state prior to the incident?
  - b) Was LAHC PHI or PII transmitted or used outside the Summit's control? If yes, describe.
  - c) What is the name of the Ransomware?
  - d) What is the name of the third-party forensic investigators referenced in your letter?
  - e) What is the status of the investigation and when will the investigators' findings be available?
  - f) What steps have been take to mitigate further risk in the future?
  - g) When can we expect a formal and final report from Summit?
  - h) Was LAHC's data fully recovered?
2. Please provide the following in writing and in compliance with the attached BAA:
- a) Why did Summit not report the Security Event to LAHC with in the appropriate timeframe?
  - b) Did the ransomware or any unauthorized program access and/or encrypt LAHC files that contained "Unsecured PHI". "Unsecured PHI" is defined as PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by DHH. 45 CFR § 164.312.
  - c) Demonstrate that there is a low probability that the "Unsecured PHI" was compromised based on a risk assessment of the following:
    - i. The nature and extent of the PHI involved (including identifiers and likelihood of re-identification);
    - ii. The unauthorized person to whom PHI disclosure was made;
    - iii. Whether the PHI was actually acquired or viewed; and
    - iv. The extent to which the risk to PHI has been mitigated. 45 CFR § 164.402.
3. Please provide the following data by 11/27/2016 (THIS SHOULD READ AS SOON AS POSSIBLE):
- a) Provide, in a secured format, a complete copy of all LAHC data stored by Summit.
  - b) Provide, in a secured format, a complete copy of all LAHC data affected by the subject security incident.

As you know, under both federal law and regulation, the ultimate responsibility for the standards, requirements and implementation of the security and privacy provisions of federal law and regulations related to PHI and PII, including all notice requirements with respect to any breach of unsecured PHI and PII, lies with LAHC. 45 CFR 164.102 et seq.

Your immediate and detailed assistance in providing the information requested (in spite of Mr. D'Antonio's deadline of November 27, 2016) will minimize the extent to which LAHC is required to make an independent investigation of the Summit data security event and provide required notice of such breach if required and will minimize Summit's responsibility under the BAA for

payment of the costs of compliance. BAA sections 2.3, 2.4, 2.5, 2.6, 2.10, 2.11, 3.1, 5.1, 5.2, 5.5 and 7.5.

I trust that it will not be necessary for LAHC to retain a third party forensic investigator to perform the detailed investigation required as to the LAHC reporting requirements flowing from the Summit data security event discovered by Summit on August 8, 2016.

I look forward to hearing from you. Thank you for your time and attention.

Sincerely,

A handwritten signature in black ink, appearing to read "Sue Buser". The signature is fluid and cursive, with the first name "Sue" and last name "Buser" clearly distinguishable.

Sue Buser

cc: Billy Bostick, Receiver, Louisiana Health Cooperative, Inc. in Rehabilitation

Philip D'Antonio, designated Privacy Officer for Louisiana Health Cooperative, Inc. in Rehabilitation



Business Associate Agreement  
Effective September 12, 2013

This Business Associate Agreement ("Agreement") effective on September 12, 2013 is entered into by and between Summit Re ("Business Associate") and Louisiana Health Cooperative, Inc. ("CO-OP").

RECITALS

CO-OP and Business Associate are parties to an agreement ("Underlying Agreement") pursuant to which Business Associate provides certain services to CO-OP and, in connection with those services, CO-OP discloses to Business Associate certain Protected Health Information ("PHI") that is subject to protection under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and Title XIII, The Health Information Technology for Economic and Clinical Health Act ("HITECH"), of the American Recovery and Reinvestment Act ("ARRA").

The parties desire to comply with the requirements set forth in the Privacy and Security Regulations and HITECH concerning the privacy of PHI.

The purpose of this Agreement is to comply with the requirements of the Privacy Rule, the Security Rule, and HITECH, including but not limited to the Business Associate Requirements at 45 C.F.R. Section 164.504(e).

Therefore, in consideration of the mutual promises and covenants contained herein, the parties agree as follows:

SECTION I – DEFINITIONS

- 1.1 Definitions. Unless otherwise provided in this Agreement, capitalized terms shall have the same meaning as set forth in the HIPAA regulations, 45 C.F.R. Sections 160 and 164, and HITECH and its related regulations.

SECTION II – OBLIGATIONS OF BUSINESS ASSOCIATE

- 2.1 Use/Disclosure of PHI. In connection with its use and disclosure of PHI, Business Associate agrees that it shall use and/or disclose PHI only as permitted or required by this Agreement or as otherwise required by law.
- 2.2 Safeguards for Protection of PHI. Business Associate agrees to use reasonable and appropriate safeguards to prevent the use or disclosure of PHI other than as provided in this Agreement, including compliance with Security Standards of the HIPAA Rules.
- 2.3 Compliance with HITECH Act and Regulations. Business associate will comply with the requirements of HITECH, codified at 42 U.S.C. §§ 17921-17954, which are applicable to Business Associate, and will comply with all regulations issued by the Department of Health and Human Services to implement these referenced statutes including but not

limited to 45 C.F.R. 164.400 - .414, as of the date by which Business Associate is required to comply with such referenced statutes and HHS regulations.

- 2.4 General Reporting. Business Associate shall report to CO-OP any use or disclosure of PHI which is not provided for by this Agreement of which Business Associate becomes aware, including breaches of unsecured PHI required by 45 C.F.R. 164.410.
- 2.5 Reporting of Breaches of Unsecured Protected Health Information. Business Associate will report in writing to CO-OP's Privacy Officer any Breach of Unsecured PHI, as defined in the Breach Notification Regulations, within 5 business days of the date Business Associate learns of the incident giving rise to the Breach. Business Associate will provide such information to CO-OP as required in the Breach Notification Regulations. To the extent a Breach is caused by Business Associate or Business Associate's subcontractors or agents, Business Associate will reimburse CO-OP for any reasonable expenses CO-OP incurs in the investigation and assessment of the Breach and obligations of notification, providing notice of the Breach to individuals, the media or the Secretary and for reasonable measures taken by CO-OP to mitigate harm to those individuals.
- 2.6 Mitigation. Business Associate shall make reasonable efforts to mitigate, to the greatest extent possible, any harmful effects arising from any improper use and/or disclosure of PHI.
- 2.7 Subcontractors. Business Associate shall ensure that any agents, including any subcontractor, that creates, receives, maintains or transmits PHI on behalf of Business Associate agrees to the same restrictions and conditions that apply to the Business Associate with respect to PHI. If Business Associate learns of Subcontractor's non-compliance with its privacy, security, reporting and other obligations relating to PHI, Business Associate shall take all steps required by the Privacy Rule, the Security Rule, and HITECH Act, including prompt notice to Covered Entity of the non compliance, reporting of an unauthorized use or disclosure of PHI, including breaches of Unsecured PHI, and taking appropriate steps to terminate the agreement with the Subcontractor or otherwise cure the noncompliance to the satisfaction of and within the time determined the Covered Entity and, as may be required under the circumstances, retrieve all PHI within the possession or control of the subcontractor for return to Business Associate or Covered Entity.
- 2.8 Access by Individuals. Business Associate shall allow individuals who are the subject of the PHI to inspect and copy their PHI maintained in a Designated Record Set in the possession of Business Associate upon instruction by the Covered Entity. If an Individual requests access to PHI contained in a Designated Record Set directly from Business Associate or its agents or subcontractors, Business Associate will notify Covered Entity in writing within 10 days of receiving such request. Business Associate agrees to promptly make any arrangement(s) for access to such PHI that Covered Entity directs.

- 2.9 Access by Department of Health and Human Services. Business Associate shall make its internal practices, books, and records relating to the use and disclosure of PHI received from or related or received by the Business Associate on behalf of the CO-OP, available to the Secretary of the Department of Health and Human Services for purposes of determining CO-OP's compliance with the HIPAA privacy regulations.
- 2.10 Access by CO-OP. Upon reasonable notice, Business Associate shall make its internal practices, book, and records relating to the use and disclosure of PHI available to CO-OP for purposes of determining Business Associate's compliance with the terms of this Agreement and Business Associate's compliance with HIPAA and HITECH.
- 2.11 Accountings of Disclosures. Business Associate agrees to document each disclosure of PHI that Business Associate creates or receives for or from Covered Entity not excepted from disclosure accounting pursuant to 45 CFR 164.528. Such accounting shall include the information necessary for CO-OP to provide an Accounting of Disclosures to any Individual who requests such an Accounting as more fully set forth in 45 CFR 164.528. If requested by CO-OP, Business Associate shall provide an accounting of disclosures directly to the requesting Individual.
- 2.12 Amendment of PHI. Business Associate agrees to make any amendment(s) to PHI maintained in a Designated Record Set that CO-OP directs or agrees to pursuant to CO-OP's obligations under the Privacy Rule. If an Individual requests an amendment of PHI maintained in a Designated Record Set directly from Business Associate or its agents or subcontractors, Business Associate must notify Covered Entity in writing within ten (10) days of receiving such request.
- 2.13 Minimum Necessary. In any instance when Business Associate uses, requests or discloses PHI under this Agreement or in accordance with other agreements that exist between Covered Entity and Business Associate, Business Associate may use or disclose only the minimum amount of PHI necessary to accomplish the intended purpose.
- 2.14 To the extent Business Associate is to carry out one or more of CO-OP's obligation(s) under the Privacy Rule (Subpart E of 45 C.F.R. Part 164), Business Associate shall comply with the requirements of the Privacy Rule Subpart E that apply to CO-OP in the performance of such obligation(s).
- 2.15 To the extent Business Associate or Business Associate Subcontractor or agent is a Group Health Plan, the Plan Documents shall provide that, except for electronic PHI disclosed to a Plan Sponsor pursuant to 45 USC 164.504(f)(1)(ii) or (iii) or as authorized under 45 C.F.R. 164.508, the Plan Sponsor will reasonably and appropriately safeguard electronic PHI created, received, maintained or transmitted to the Plan Sponsor on behalf of the Group Health Plan, including
- a. implementing administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of electronic PHI that it creates, receives, maintains or transmits on behalf other group health plan;

- b. ensure that adequate separation required by 45 USC 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures;
- c. ensure that any agent to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and
- d. reports to the group health plan any security incident of which it becomes aware.

### SECTION III – PERMITTED USES AND DISCLOSURES

- 3.1 General. Except as otherwise limited in this Agreement, Business Associate may use or disclose PHI to perform functions, activities, or services for, or on behalf of, CO-OP as specified in the Underlying Agreement, provided that such use or disclosure would not violate the Privacy Rule if done by CO-OP.

Business Associate may use PHI it creates or receives for or from Covered Entity as necessary for Business Associate to carry out Business Associate's proper management and administration or to carry out the legal responsibilities of the Business Associate and may disclose PHI received in its capacity as a Business Associate for such purposes if required by law or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or disclosed only as required by law or for the purpose for which it was disclosed to the person and the person notifies the business associate of any instances in which it is aware in which the confidentiality of the information has been breached.

### SECTION IV – OBLIGATIONS OF CO-OP

- 4.1 Notice of Privacy Practices. CO-OP has included and will continue to include, in the CO-OP Notice of Privacy Practices information advising Individuals that CO-OP may disclose their PHI to Business Associates.
- 4.2 Consents/Authorizations. CO-OP has obtained and will continue to obtain, from Individuals, consents, authorizations and other permissions that may be required by the Privacy Rule or applicable state laws and/or regulations prior to furnishing Business Associate PHI pertaining to Individuals.
- 4.3 Restrictions. CO-OP will promptly notify Business Associate in writing of any restrictions on the use and disclosure of PHI about Individuals that CO-OP has agreed to that may affect Business Associate's ability to perform its obligations under the Underlying Agreement or this Agreement.
- 4.4 Revocation of Authorization. CO-OP shall promptly notify Business Associate in writing of any change in, or revocation of, permission by an Individual to use or disclose PHI, if such changes or revocation may affect Business Associate's ability to perform its obligations under the Underlying Agreement or this Agreement.

## SECTION V – SECURITY

- 5.1 Business Associate agrees to implement the Security Rule (security standards as set out in 45 C.F.R. parts 160, 162 and 164), Administrative, Physical and Technical Safeguards that reasonably and appropriately protect the Confidentiality, Integrity, and Availability of the electronic PHI that Business Associate creates, receives, maintains, or transmits on behalf of the Covered Entity.
- 5.2 Business Associate agrees to report to Covered Entity any security incident within 5 business days of when Business Associate becomes aware of such incident, including breaches of unsecured PHI as required by 45 CFR 164.410.
- 5.3 Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides PHI received from, or created or received by, Business Associate on behalf of Covered Entity agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such PHI.
- 5.4 Business Associate will ensure that any agent, including a subcontractor, to whom it provides electronic Protected Health Information agrees to implement the Security Rule, Administrative, Physical and Technical Safeguards that reasonably and appropriately protect the Confidentiality, Integrity, and Availability of the electronic PHI.
- 5.5 Business Associate agrees to make its policies, procedures, and documentation relating to the safeguards described herein available to the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Security Rule.

## SECTION VI – TERM & TERMINATION

- 6.1 Term and Termination. This Agreement shall be effective as of the Effective Date and shall terminate when all of the PHI provided by CO-OP to Business Associate, or created or received by Business Associate on behalf of CO-OP, is destroyed or returned to CO-OP. The parties acknowledge and agree that the terms and conditions stipulated in this Agreement shall apply to any future written or oral agreements between CO-OP and Business Associate which require the disclosure of PHI, whether or not this Agreement is incorporated by reference into future agreements executed between the parties.
- 6.2 Termination for Cause. CO-OP may terminate this Agreement if CO-OP determines that Business Associate has breached a material term of this Agreement. Alternatively, CO-OP may choose to provide Business Associate with notice of the existence of an alleged material breach and provide Business Associate an opportunity to cure the alleged material breach within the time specified by CO-OP. In the event Business Associate fails to cure the breach to the satisfaction of CO-OP, CO-OP may immediately terminate this Agreement.

Business Associate may terminate this Agreement if Business Associate determines that CO-OP has breached a material term of this Agreement. Alternatively, Business

Associate may choose to provide CO-OP with notice of the existence of an alleged material breach and provide CO-OP an opportunity to cure the alleged material breach within the time specified by Business Associate. In the event CO-OP fails to cure the breach to the satisfaction of Business Associate, Business Associate may immediately terminate this Agreement.

- 6.3 Effect of Termination. Upon termination of this Agreement, for any reason, Business Associate shall, if feasible, return or destroy all of the PHI that Business Associate still maintains in any form and shall not retain any copies of such PHI. If such return or destruction is not feasible, Business Associate shall extend the protections of this Agreement to the PHI and shall limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible, including the following:
- Retain only that which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities or which makes the return or destruction infeasible;
  - Return or destroy the remaining PHI that the Business Associate still maintains in any form based upon consultation and instruction by CO-OP;
  - Continue to use appropriate safeguards and comply with Subpart C of 45 C.F.R. Part 164 with respect to electronic PHI to prevent use or disclosure of the PHI other than as provided for in this Section, for as long as Business Associate retains the PHI;
  - Not use or disclose PHI retained by Business Associate other than for the purposes for which such PHI was retained and subject to the same conditions set out at Sections II and III which applied prior to termination; and
  - Return or destroy PHI retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration, to carry out its legal responsibilities or other condition which makes return or destruction infeasible based upon consultation and instruction by CO-OP.
  - Return or destroy PHI created, received or maintained by Business Associate subcontractors based on consultation and instruction by CO-OP.

#### SECTION VII – MISCELLANEOUS

- 7.1 Amendment. The Parties agree to take such action as is necessary to amend this agreement from time to time as is necessary for compliance with the requirements of the HIPAA rules and any other applicable law. Notwithstanding, this Agreement shall be deemed to amend automatically, by force of law and without further act of the parties, if necessary to bring the Agreement into compliance with any changes in HIPAA, HITECH or any related regulations that are made after the date of execution of this Agreement.
- 7.2 Interpretation. Any ambiguity in this Agreement shall be resolved in a manner that brings the Agreement into compliance with the then most current version of HIPAA regulations, 45 C.F.R. Sections 160 and 164 and HITECH and its related regulations.
- 7.3 No Third Party Beneficiaries. Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any other person other than the parties and their respective successors or assigns, any rights, remedies, obligations or liabilities

whatsoever.

- 7.4 Notice: Any notice required to be provided pursuant to this Agreement shall be made as follows:

To CO-OP: CO-OP's Privacy Officer  
Louisiana Health Cooperative, Inc.  
3445 North Causeway Boulevard, Suite 800  
Metairie, LA 70002

To Business Associate:  
Summit Reinsurance Services, Inc.  
7030 Pointe Inverness Way, Suite 350  
Fort Wayne, IN 46804

- 7.5 Indemnification: Business Associate shall defend, hold harmless and indemnify CO-OP and its employees, agents, officers, directors, members, contractors, and subsidiary and affiliate entities, from and against any claims, losses, damages, liabilities, costs, expenses, penalties or obligations (including reasonable in-house and external attorneys' fees) arising from any action, suit, or proceeding resulting from a negligent act, omission or failure to comply with the terms of this Business Associate Agreement caused by Business Associate or Business Associate's subcontractors or agents. This indemnity shall not be enforceable if the damage or award is determined to result solely from, or is caused in part by a negligent act or omission of CO-OP or CO-OP affiliated Provider/Practitioner, or agents.

CO-OP shall indemnify, defend and hold harmless Business Associate from and against any claims, costs, losses, liability or expenses (including reasonable attorney's fees) arising from any action, suit, or proceeding resulting from a negligent act, omission or failure to comply with the terms of this Business Associate Agreement on the part of CO-OP. This indemnity shall not be enforceable if the damage or award is determined to result solely from, or is caused in part by a negligent act or omission of Business Associate or Business Associate's subcontractor or agents.

- 7.6 Insurance. In support of its obligation to indemnify CO-OP, the Business Associate will maintain, during the term of this Agreement and for a period of three (3) years beyond its termination, privacy and cyber liability coverage covering damages including costs of mitigation and reporting accruing as a result of malicious code, unauthorized access or unauthorized use, extortion, hacking or administrative or operational mistakes with a minimum limit of \$1,000,000 each incident and an aggregate limit of \$3,000,000 covering Business Associate's obligations to the Covered Entity under this Business Associate Agreement.

IN WITNESS WHEREOF, the parties hereto have duly executed this Agreement on the dates set

forth below.

CO-OP

By: 

Title: C.E.O.

Date: 9/13/2013

(Business Associate) Summit Insurance Services, Inc.

By: 

Title: PRESIDENT

Date: 9-10-13



# Burglass Tankersley

Attorneys at Law  
5213 Airline Drive  
Metairie, Louisiana 70001-5602  
www.burglass.com

Sue Buser  
sbuser@burglass.com

Direct Dial  
(504) 836-0460  
Direct Fax  
(504) 287-0460

November 3, 2016

Sian Schafle  
Alexandra Bradley  
Mullen Coughlin, LLC  
1275 Drummers Lane, Suite 302  
Wayne, PA 19087

by email to [sschafle@mullen.legal](mailto:sschafle@mullen.legal)  
by email to [abradey@mullen.legal](mailto:abradey@mullen.legal)

RE: *James J. Donelon, Commissioner of Insurance for the State of Louisiana v. Louisiana Health Cooperative, Inc. ("LAHC"), 19<sup>th</sup> JDC #641 928, Section 26*  
Second Request for all LAHC records and data  
Our File #: 87004

Dear Ms. Schafle and Ms. Bradley:

It was a pleasure speaking to both of you regarding issues related to the October 27, 2016 notice of the Summit Reinsurance Services, Inc. ("Summit Re") data security breach discovered by Summit Re on August 8 2016.

To recap our discussions, you indicated that:

- 1) Summit Re retained your firm to conduct an investigation of a data security breach at Summit Re, but that Summit Re has not yet retained its own expert or undertaken to obtain a report on the unauthorized remote access to a Summit server via a Brute Force attack and the ransomware attack, both referred to herein as the "Security Breach."
- 2) Your firm retained Charles River Associates, with a team formerly associated with Navigant Consultants, to conduct a forensic investigation into the Summit Re data security breach and that the findings of that investigation were provided in October 2016.
- 3) Neither your firm, Charles River Associates, and/or Summit Re have requested and/or provided a report as to the Summit Re Security Breach.
- 4) It is possible that Summit Re may retain its own expert to provide a report on the Summit Re Security Breach.
- 5) Summit Re made the decision to disclose the Security Breach on the Summit Re server to LAHC because of the possibility of access to LAHC data and information. The unauthorized direct server access via brute force attack was not initially disclosed to LAHC.
- 6) While there has been no determination at present as to whether LAHC data was encrypted by the ransomware attack, Summit Re is continuing its investigation into this and may be able to provide additional information.

{00578287 - v1}

- 7) Summit Re has agreed to pay the costs of printing and mailing written notice to affected individuals (required to be made within sixty (60) days of LAHC's discovery of the breach), advertising, website posting, call center activity, maintenance of the required logs and records, and credit monitoring. 45 CFR 164.404.

If you believe that any of these statements are inaccurate or incomplete, please identify any inaccuracies or omissions and provide a brief statement of your position.

As to the findings of the Charles River Associates investigation, you indicated that:

- 1) Charles River Associates determined that a Summit data server was remotely accessed by an unauthorized person or program using a Brute Force attack on the server's RDP (Remote Desktop Protocols), gaining access via an existing Summit domain user account.
- 2) Upon unauthorized entry to the server, ransomware was manually executed on the Summit Re data server, which began the process of encrypting data in an effort to extort payment by preventing Summit from accessing its own data.
- 3) The ransomware was determined to be XTBL/troldesh.
- 4) This ransomware attack was limited to a single Summit Re server.
- 5) This ransomware attack was limited to a single user account, which was not an administrator account, but which had domain access.
- 6) The brute force ransomware attack permitted an unidentified person or persons to obtain remote access to the Summit Re server.
- 7) The affected server contained LAHC data and information, which included LAHC claim files with Protected Health Information ("PHI") and Personal Identifying Information ("PII") of LAHC.
- 8) The LAHC data and information was not encrypted by Summit Re at the time of the attack.
- 9) When the ransomware began encrypting the single Summit Re server, Summit Re was able to stop the process by taking the server offline.
- 10) Investigation revealed that the ransomware encryption had not moved laterally.
- 11) Summit Re was able to restore the LAHC data and information.
- 12) The investigation did not show any evidence that LAHC data was exported, transmitted or used outside the control of Summit Re.
- 13) The Charles River Associate forensic investigation determined that LAHC data and information was impacted by the Security Breach.
- 14) While there is no forensic evidence found by Charles River Associates that LAHC data and information was affected in the Security Attack, your firm, Charles River Associates and/or Summit Re cannot rule out that LAHC data was transmitted and/or used outside of Summit Re's control as a result of the Security Attack and cannot say definitively that nothing happened.
- 15) There has been no determination at present as to whether LAHC data and information was encrypted by the ransomware attack.

If you believe that any of these statements are inaccurate or incomplete, please identify any inaccuracies or omissions and provide a brief statement of your position.

As a follow up to our phone conference on November 2, 2016, LAHC would like to formally request that Summit Re provide the following:

- 1) Provide a complete copy of all LAHC data and information stored by Summit.
- 2) Provide a complete copy of all LAHC data and information stored on the affected server identified by Charles River Associates as the only server affected by the ransomware brute force attack.
- 3) Provide a complete copy of the LAHC data and information that was impacted by the ransomware brute force attack.
- 4) Provide complete information as to what LAHC data was encrypted by the brute force ransomware attack.
- 5) Provide LAHC with any and all information as to whether the single domain user identified by the Summit Re investigation had access to LAHC data and information.
- 6) Provide a complete written report as to the steps Summit Re has taken to mitigate further risk.
- 7) Confirm in writing that the LAHC data and information was fully recovered.
- 8) Provide a complete report on the brute force ransomware attack which fully addresses each of the following:
  - a) Was LAHC PHI or PII stored in an encrypted state on the affected Summit Re server?
  - b) Was LAHC PHI or PII accessed by the Security Event?
  - c) Was LAHC PHI or PII encrypted by the Security Event?
  - d) Was LAHC PHI or PII transmitted or used outside Summit Re's control?
  - e) Was the LAHC data fully recovered?
  - f) A detailed listing of the results of the Summit Re forensic investigation.
  - g) The reason why Summit Re did not report the Security Event to LAHC within five (5) days of discovery of the incident.
  - h) The reason why Summit Re did not report the Security Event to LAHC within sixty (60) days of discovery of the incident.
  - i) The steps taken by Summit Re to mitigate further risk.
- 9) Demonstrate that there is a low probability that LAHC PHI or PII was compromised based on:
  - a) The nature and extent of the LAHC PHI or PII involved (including identifiers and the likelihood of re-identification);
  - b) The unauthorized person to whom LAHC PHI or PII disclosure was made;
  - c) Whether LAHC PHI or PII was actually acquired or viewed; and
  - d) The extent to which the risk to LAHC PHI or PII has been mitigated.

To the extent Summit Re is unwilling and/or unable to fully report on this incident, LAHC will have no choice but to undertake an independent forensic investigation at Summit Re's expenses, pursuant to section 2.5 of the Business Associate Agreement with LAHC, to comply with the federal and state reporting requirements under the Patient Protection and Affordable Care Act (ACA), the Health Insurance Portability and Accountability Act (HIPAA) and any other applicable statute or regulation.

LAHC asks that you remind Summit Re that the Business Associate Agreement ("BAA") with LAHC requires that Summit Re to provide LAHC with a written report of any breach of unsecured PHI and/or PII within five (5) business days of the date Summit learned of the incident. We request that Summit Re provide the required report with specific detail and findings.

The BAA, section 2.5, also requires Summit Re to reimburse LAHC for all reasonable expense in the investigation and assessment of the breach, the obligations of reporting and notification to individuals,

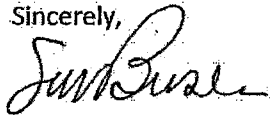
the media or the Secretary of the Department of Health and Human Services ("DHH"), and for LAHC's mitigation efforts.

LAHC trusts that an independent separate investigation into the Summit Re security breach will not be required and that Summit Re will provide the complete information and reporting required. However, if Summit Re does not or can not provide satisfactory information in a timely manner, it may be necessary for LAHC to obtain a forensic investigation and/or conduct an on site visit in the immediate future to allow time for LAHC to meet its reporting requirements.

The clock is ticking and time is of the essence for LAHC to make a determination of LAHC's reporting responsibilities.

I look forward to discussing this further at the scheduled phone conference on Monday November 14, 2016. Thank you for your time and attention.

Sincerely,



Sue Buser

cc: Billy Bostick, Receiver, Louisiana Health Cooperative, Inc. in Rehabilitation  
Philip D'Antonio, LAHC Security Officer

## Sue A. Buser

---

**From:** Alex Bradley <[abradley@mullen.legal](mailto:abradley@mullen.legal)>  
**Sent:** Wednesday, November 09, 2016 8:10 AM  
**To:** Philip@DTec.us; Sue A. Buser  
**Cc:** Sian Schafle; Hannah Keem  
**Subject:** Summit - LAHC

Hi Sue & Phil,

Per your request, please allow this email to memorialize Summit's offer to assist your organization in providing notification to those individuals whose information was stored on the impacted server. As we indicated on our Monday call, Summit will provide the following notification services to potentially impacted individuals:

- Written notification of this incident
- An offer of access to credit monitoring at no cost to the individuals (cost to be covered by Summit)
- Call center support to respond to inquiry from potentially impacted population

Thank you,

Alex

**Alexandra Bradley**  
**Attorney**  
**Mullen Coughlin LLC**  
1275 Drummers Lane, Suite 302  
Wayne, PA 19087  
(267) 930-4773 – office  
(410) 404-3631 – mobile  
[abradley@mullen.legal](mailto:abradley@mullen.legal)



MULLEN  
COUGHLIN

This email may be an attorney-client communication or otherwise confidential and privileged. If you are not the intended recipient, or received it in error, do not review or copy. Please immediately notify the sender and permanently delete/destroy the email and attachments.

# Burglass Tankersley

Attorneys at Law  
5213 Airline Drive  
Metairie, Louisiana 70001-5602  
www.burglass.com

Sue Buser  
sbuser@burglass.com

Direct Dial  
(504) 836-0460  
Direct Fax  
(504) 287-0460

November 15, 2016

Matthew K. Lynch by email to [matt.lynch@oig.hhs.gov](mailto:matt.lynch@oig.hhs.gov)  
Director of the Insurance Programs Group  
Center for Consumer Information and Insurance Oversight (CCIIO)  
Centers for Medicare and Medicaid Services (CMS)  
200 Independence Avenue, S.W.  
Washington, DC 20201

Kevin Counihan by email to [Kevin.counihan@cms.hhs.gov](mailto:Kevin.counihan@cms.hhs.gov)  
Chief Executive Officer, Health Insurance Marketplace  
Director, Center for Consumer Information and Insurance Oversight  
Department of Health & Human Services  
Centers for Medicare & Medicaid Services  
200 Independence Avenue SW  
Washington, DC 20201

AND BY OVERNIGHT DELIVERY

RE: *James J. Donelon, Commissioner of Insurance for the State of Louisiana v. Louisiana Health Cooperative, Inc. ("LAHC")*, 19<sup>th</sup> JDC #641 928, Section 26  
Summit Re Data Security Event of August 8, 2016  
Our File #: 87004

## REPORT OF DATA SECURITY BREACH

Dear Mr. Lynch and Mr. Counihan:

As you and I have previously discussed, this firm has been retained to represent the interests of Louisiana Health Cooperative, Inc. in Rehabilitation ("LAHC").

LAHC received notice on October 27, 2016 that on August 8, 2016 LAHC's reinsurance **BROKER?** For commercial reinsurance for the 2014 Plan Year, Summit Reinsurance Services, Inc. ("Summit Re") discovered "that ransomware had infected a server containing personal information that Summit Re determined may consist of one or more of the following data elements: member names, provider names, Social Security numbers, health insurance information, and some claim-focused medical records containing information such as diagnosis/clinical information." A copy of the October 24, 2016 letter to LAHC from Summit Re is attached as **Exhibit A**.

LAHC worked with the attorneys for Summit Re to attempt to determine whether the Summit Re data security breach triggered the reporting requirements of the applicable provisions of the Patient Protection and Affordable Care Act ("ACA") and the implementing sections of the Code of Federal Regulations ("CFR"), the Health Insurance Portability and Accountability Act ("HIPAA"), Louisiana law, including, but not limited to, La. R.S. 51:3071, et seq., and any other such statutory requirements as to a breach of unsecured protected health information ("PHI") and personally identifiable information ("PII") (all collectively the "Security and Privacy Laws"). But to date, LAHC has not been able to do so as Summit Re has provided very little information and no expert analysis or reporting on the details and Summit Re findings. Summit Re has provided LAHC with a spreadsheet of 12,676 LAHC members whose information may have been compromised which is available upon request. Summit Re has also offered to provide the following notification services to potentially impacted individuals:

- Written notification of this incident
- An offer of access to credit monitoring at no cost to the individuals (cost to be covered by Summit)
- Call center support to respond to inquiry from potentially impacted population

Because LAHC has no information as to the details of the Summit Re data security breach, LAHC has made demand on Summit Re to fully comply in all respects with the requirements of all state and federal laws and regulations, including, but not limited to the Health Insurance Portability and Accountability Act ("HIPAA"), the Patient Protection and Affordable Care Act ("ACA") (including 42 USC 17921-17954) and related federal regulations, such as 45 CFR 160 and 45 CFR 164, Title XIII, the Health Information and Clinical Health Act ("HITECH"), and Louisiana law, including, but not limited to La. R.S. 51:3071, et seq. See the letter to Summit Re's attorneys attached as **Exhibit B**.

Summit Re can be contacted through the attorneys as follows:

Sian Schafle  
Alexandra Bradley  
Mullen Coughlin, LLC  
1275 Drummers Lane, Suite 302  
Wayne, PA 19087

by email to [sschafle@mullen.legal](mailto:sschafle@mullen.legal)  
by email to [abradey@mullen.legal](mailto:abradey@mullen.legal)

Or directly through:

Attention: Mark Troutman  
President  
Summit Reinsurance Services, Inc.  
7030 Pointe Inverness Way, Suite 350  
Fort Wayne, IN 46804

If further action is needed on the part of LAHC, please let me know at your earliest convenience.

Should you have any questions or need further information, please feel free to contact me.

Thank you for your time and attention.

Sincerely,



Sue Buser

cc: Billy Bostick, Louisiana Health Cooperative, Inc. in Rehabilitation  
Assistant Louisiana Attorney General Michael Guy  
Terrance Mebane (by email to [terrance.a.mebane@usdoj.gov](mailto:terrance.a.mebane@usdoj.gov))  
Mark Troutman, Summit Reinsurance Services, Inc.  
Louisiana Department of Insurance